



Kings Langley School

Unlocking Potential for Life

Privacy Notice for Students



CONTENTS

1. Privacy Notice

Page 3 - 12



KINGS LANGLEY SCHOOL

PRIVACY NOTICE FOR STUDENTS

Kings Langley School (called the Data Controller) collects data and information about our pupils (called the Data Subjects) so that we can run effectively as a school. This privacy notice explains how and why we collect pupils' data, what we do with it and what rights parents and pupils have.

The categories of pupil information that we collect, hold and share include:

- Personal information (such as name, unique pupil number and address);
- Characteristics (such as ethnicity, language, medical conditions, and free school meal eligibility);
- Biometric data about pupils (for Cashless catering, printing and library systems.
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Assessment information (such as grades, targets, and teachers comments for pupil reports)
- Examinations information (such as Unique Candidate number, internal and public examination entries and results)
- Medical information (such as Doctor details, medical conditions, medication, medical history, allergy / dietary information)
- Special educational needs information (such as Learning Needs classification, support needed, review information)
- Behavioural information (such as Achievement and Behaviour incidents, detentions recorded, exclusions information)
- Learning information (such as courses studied, timetables, class groups, Post 16 learning information in the Sixth form)
- Welfare information (such as adoption / care information, child protection information)
- Contact information (such as telephone, e mail and postal addresses of emergency and parental contacts of the pupil)

Why do we collect and use pupil information?

We collect and use pupil information under section 537A of the Education Act 1996, section 83 of the Children Act 1989, and to carry out tasks in the public interest. If we need to collect special category (sensitive) personal information, we rely upon reasons of substantial public interest (equality of opportunity or treatment).

We collect and use pupil information under the following lawful bases under the UK General Data Protection Regulation (UK GDPR):

- a. where we have the consent of the data subject [Article 6 (a)];
- b. where it is necessary for compliance with a legal obligation [Article 6 (c)];
- c. where processing is necessary to protect the vital interests of the data subject or another person [Article 6 (d)];
- d. where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller [Article 6 (e)].



Where the personal data we collect about pupils is sensitive (i.e. special category) personal data, we will only process it where:

- a. we have explicit consent [Article 9 (2)(a)];
- b. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent [Article 9 (2)(c)]; and / or
- c. processing is necessary for reasons of substantial public interest, and is authorised by UK law (see section 10 of the 2018 Data Protection Act) [Article 9 (2)(g)].

Please see our Data Protection Policy on the school web site for a definition of sensitive personal data.

We use the pupil data to support our statutory functions of running a school, in particular:

- to decide who to admit to the school;
- to maintain a waiting list;
- to support pupil learning;
- to monitor and report on pupil attainment progress;
- to provide appropriate pastoral care;
- to assess the quality of our services;
- to comply with the law regarding data sharing;
- for the protection and welfare of pupils and others in the school;
- for the safe and orderly running of the school;
- to promote the school;
- to communicate with parents / carers.

The categories of pupil information that we collect, hold and share include:

- a. Personal information (such as name, unique pupil number and address);
- b. Characteristics (such as ethnicity, language, medical conditions and free school meal eligibility);
- c. Attendance information (such as sessions attended, number of absences and absence reasons)

From time to time and in certain circumstances, we might also process personal data about pupils, some of which might be sensitive personal data, including information about criminal proceedings / convictions, information about sex life and sexual orientation, child protection / safeguarding. This information is not routinely collected about pupils and is only likely to be processed by the school in specific circumstances relating to particular pupils, for example, if a child protection issue arises or if a pupil is involved in a criminal matter. Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

We collect information about pupils when they join the school and update it during their time on the roll as and when new information is acquired.

As the school has a cashless catering system, we also process biometric data about pupils. Please see our Data Protection Policy for more details about how we process biometric data.



Collecting pupil information

Whilst the majority of pupil information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the UK GDPR, we will inform you whether you are required to provide certain pupil information to us or if you have a choice in this. Where appropriate, we will ask parents / pupils (Year 8 and above) for consent to process personal data where there is no other lawful basis for processing it, for example where we wish to use photos or images of pupils on our website, in our school prospectus or on social media to promote school activities. Parents / pupils (Year 8 and above) may withdraw consent at any time by contacting the Data Protection Officer at the school.

In addition, the School uses CCTV cameras around the school site for security purposes and for the protection of staff and pupils. CCTV footage may be referred to during the course of disciplinary procedures (for staff or pupils) or to investigate other issues. CCTV footage involving pupils will only be processed to the extent that it is lawful to do so. Please see our CCTV policy for more details.

Storing pupil data

We hold pupil data securely and have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. Access to information is limited to those who have a business need to know it and who are subject a duty of confidentiality. A significant amount of personal data is stored electronically, for example, on our MIS database. Some information may also be stored in hard copy format.

Data stored electronically may be saved on a cloud based system which may be hosted in a different country.

Personal data may be transferred to other countries if, for example, we are arranging a school trip to a different country. Appropriate steps will be taken to keep the data secure.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach involving your data where we are legally required to do so.

When a pupil moves to another educational setting or school phase, the vast majority of information that we hold will move to that setting, although we may need to retain a certain amount of personal data, as laid out in our Data Retention Policy and Schedule [available on request].

Where we act as the final setting in a student's education, we are required to retain some personal information for a period after they have left. Typically that information will be retained until they reach the age of 25, after which it may be archived or securely destroyed. There may be reasons for retaining data longer than this, which are laid out in our Data Retention Policy and Schedule.

Who do we share pupil information with?

We routinely share pupil information with:

- education settings that pupils attend after leaving us;
- our local authority Hertfordshire County Council;



- a pupil's home local authority (if different);
- commissioned providers of local authority services [e.g. Herts for Learning Ltd]
- the Department for Education (DfE);
- school governors / trustees;
- exam boards;

From time to time, we may also share pupil information with other third parties including the following:

- the Police and law enforcement agencies;
- NHS health professionals including the school nurse, educational psychologists,
- Education Welfare Officers;
- Courts, if ordered to do so;
- the National College for Teaching and Learning;
- the Joint Council for Qualifications;
- Prevent teams in accordance with the Prevent Duty on schools;
- other schools, for example, if we are negotiating a managed move and we have your consent to share information in these circumstances;
- our HR providers, for example, if we are seeking HR advice and a pupil is involved in an issue;
- UCAS
- our legal advisors;
- our insurance providers / the Risk Protection Arrangement;

Some of the above organisations may also be Data Controllers in their own right in which case we will be joint controllers of your personal data and may be jointly liable in the event of any data breaches.

We may also share pupil data with a number of providers of software tools which may be used to: support pupil learning; monitor and report on pupil attainment and progress; deliver the educational curriculum; ensure the safety and wellbeing of pupils; communicate with parents; or to carry out other operational processes to support our core activities as a public authority, under Article 6(e) of the UK GDPR. [A full list of these providers is available on request.] These providers act as data processors on our behalf, and are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow them to use your personal data for their own purposes, and we only permit them to process your personal data for specified purposes and in accordance with our instructions.

In the event that we share personal data about pupils with third parties or data processors, we will provide the minimum amount of personal data necessary to fulfil the purpose for which we are required to share the data. Where necessary, we will carry out a Data Protection Impact Assessment (DPIA) to assess any risks involved.

Aged 14+ qualifications

For pupils enrolling for post 14 qualifications, the information you supply is used by the Learning Records Service (LRS). The LRS issues Unique Learner Numbers (ULN) and creates Personal Learning records across England, Wales and Northern Ireland, and is operated by the Education and Skills Funding Agency, an executive agency of the Department for Education (DfE). The LRS will give us a pupil's ULN and may also give us details about the pupil's learning or qualifications. For more information about how your information is processed, and to access your Personal Learning Record,



please refer to: <https://www.gov.uk/government/publications/lrs-privacy-notice/lrs-privacy-notice#tier-2-privacy-notice-text>

Why we share pupil information

We do not share information about our pupils with anyone without consent unless the law allows us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our pupils with the (DfE) under regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

Data collection requirements:

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers
- post-16 education and training providers

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / pupil once he/she reaches the age 16.

Our pupils aged 16+

We will also share certain information about pupils aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers;
- youth support services;
- careers advisers.

For more information about services for young people, please visit our [local authority website](#).



The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department. It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

We are required by law, to provide information about our pupils to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

To find out more about the pupil information we share with the department, for the purpose of data collections, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

To find out more about the NPD, go to: <https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information>.

The department may share information about our pupils from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The DfE has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data;
- the purpose for which it is required;
- the level and sensitivity of data requested; and
- the arrangements in place to store and handle the data.

To be granted access to pupil information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

For more information about the department's data sharing process, please visit: <https://www.gov.uk/data-protection-how-we-collect-and-share-research-data>

For information about which organisations the department has provided pupil information, (and for which project), please visit the following website: <https://www.gov.uk/government/publications/national-pupil-database-requests-received>

To contact DfE: <https://www.gov.uk/contact-dfe>



Requesting access to your personal data

Under data protection legislation, pupils, and in some circumstances, parents, have the right to request access to information about them that we hold ("Subject Access Request"). From the age of 13, we generally regard pupils as having the capacity to exercise their own rights in relation to their personal data. This means that where we consider a pupil to have sufficient maturity to understand their own rights, we will require a Subject Access Request to be made by the pupil and not their parent(s) on their behalf. This does not affect any separate statutory right parents might have to access information about their child.

Subject to the section below, the legal timescales for the School to respond to a Subject Access Request is one calendar month. As the School has limited staff resources outside of term time, we encourage parents / pupils to submit Subject Access Requests during term time and to avoid sending a request during periods when the School is closed or is about to close for the holidays. This will assist us in responding to your request as promptly as possible. [For further information about how we handle Subject Access Requests, please see our Data Protection Policy].

Parents of pupils who attend academies have a separate statutory right to receive an annual written report setting out their child's attainment for the main subject areas which are taught. This is an independent legal right of parents rather than a pupil's own legal right which falls outside of the UK GDPR, therefore a pupil's consent is not required even if a pupil is able to make their own decisions in relation to their personal data, unless a court order is in place which states otherwise.

The term "parent" is widely defined in education law to include the natural or adoptive parents (regardless of whether parents are or were married, whether a father is named on a birth certificate or has parental responsibility for the pupil, with whom the pupil lives or whether the pupil has contact with that parent), and also includes non-parents who have parental responsibility for the pupil, or with whom the pupil lives. It is therefore possible for a pupil to have several "parents" for the purposes of education law.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress;
- prevent processing for the purpose of direct marketing;
- object to decisions being taken by automated means;
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of our data protection responsibilities.

We will always seek to comply any requests regarding your rights, however please note that we may still be required to hold or use your information to comply with legal duties.

For further information about your rights, including the circumstances in which they apply, see the [guidance](#) from the Information Commissioners Office (ICO) on individuals' rights under the UK GDPR.

If you have a concern about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at <https://ico.org.uk/concerns/>



Contact:

You can contact the Information Commissioners Office on 0303 123 1113 or via email <https://ico.org.uk/global/contact-us/email/> or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

If you would like to discuss anything in this privacy notice, please contact:

- Mrs E Hughes, Database and Admissions Coordinator.
- Mrs D Bell, Data Protection Officer

E Mail address: admin@kls.herts.sch.uk

Changes to this Privacy Notice

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Addendum to Privacy Notice

Privacy Notice Coronavirus Test and Trace

The development of the NHS Test and Trace scheme is a key part of the government's plan to manage Coronavirus. As a private individual, compliance with the scheme may be optional, so that an individual cannot be forced to provide details when visiting some types of establishments. However, schools are public authorities and have a legal duty to protect and promote the welfare of pupils, as well as a duty of care to staff. We are required to manage confirmed cases of coronavirus (COVID-19) amongst the school community to contain any outbreak by engaging with the NHS Test and Trace process and by following local health protection team advice.

If a person in a school has COVID-19 or symptoms of the virus they will be sent home, as will other people in school who have had contact with this individual and who may be at risk. In a school setting, it is unlikely that any one individual will know the details of others around them who may have been affected. It is only the school that will have that data. We would notify individuals about a risk, and in many instances that will be sufficient.

However, the Department for Education guidance says:

'As part of the national test and trace programme, if other cases are detected within the child or young person's cohort or in the wider education or childcare setting, Public Health England's local Health Protection Teams will conduct a rapid investigation and will advise schools and other settings on the most appropriate action to take.'

If a case or suspected case of Coronavirus arises in our school then it may be necessary for us to share contact data of employees, pupils/students, contractors or visitors with NHS Test and Trace workers in order to make the process as effective as possible. Although at no point will we share data without a sound legal basis, in this situation it is not a matter of giving consent to share data, as there is a Public Duty to do so. This data will usually only consist of names and contact details, e.g. email address and/or telephone number.



We will therefore be sharing data on the basis that this is a Public Duty and, in the case of any health data, that it is necessary for the public interest, as set out below. It will only be used and retained in line with national guidelines and the applicable data protection laws. Where data needs to be shared we will:

- only share data with the relevant authorities
- verify the identity of persons requesting personal data
- limit the data shared to the minimum necessary
- ensure the data is kept secure, and only share via secure methods
- keep a record of the data shared, under the strictest confidence
- notify any individuals whose data has been shared (where possible)

NHS Test and Trace and the Law

The law on protecting personally identifiable information, known as the General Data Protection Regulation (GDPR), allows Public Health England to use the personal information collected by NHS Test and Trace. The section of the GDPR that applies is:

Article 6(1)(e) – ‘processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller’

As information about health is a special category of personal information, a further section of the GDPR applies:

Article 9(2)(i) – ‘processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare’

Public Health England also has special permission from the Secretary of State for Health and Social Care to use personally identifiable information without people’s consent where this is in the public interest. This is known as ‘Section 251’ approval and includes the use of the information collected by NHS Test and Trace to help protect the public from coronavirus. The part of the law that applies here is Section 251 of the National Health Service Act 2006 and the associated Health Service (Control of Patient Information) Regulations 2002.

The privacy notice for the service can be found here:

<https://contact-tracing.phe.gov.uk/help/privacy-notice>

Rights of Data Subjects in relation to their personal data

Any data subject has the right to request access to personal data that we hold about them. To make a request for access to their personal data, individuals should contact our DPO.

Individuals also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed

If you have a concern about the way we are collecting or using your personal data, you should raise



your concern with our DPO in the first instance. You can also contact the Information Commissioner's Office, if necessary, at <https://ico.org.uk/concerns/>

Contact:

If you would like to discuss anything in this privacy notice, please contact:
Diane Bell, Deputy Head (School Manager), Data Protection Officer

This Privacy Notice should be read alongside the other GDPR and Data Protection documents on our website.